AWS Cloud Management Tools Competency

Technology Partner Validation Checklist

September 2018
Version 1.0

Table of Contents

Introduction

The goal of the AWS Competency Program is to recognize APN Partners who demonstrate technical proficiency and proven customer success in specialized solution areas. The Competency Partner Validation Checklist ('checklist') is intended for APN Partners who are interested in applying for an AWS Competency. The checklist provides the criteria necessary to achieve the designation under the AWS Competency Program. APN Partners undergo a validation of their capabilities upon applying for the specific Competency. AWS reserves the right to make changes to this document at any time.

AWS Cloud Management Tools Competency Program

AWS Cloud Management Tools (CMT) Competency Partners provide solutions targeting one or more of the use cases in managing AWS infrastructure including: Cloud Governance and Resource & Cost Optimization. These specialized software solutions enable companies to properly manage and govern their AWS workloads while maintaining speed, agility, resiliency and cost benefit the cloud provides.

Expectations of Parties

It is expected that APN Partners will review this document in detail before submitting an application for the AWS Competency Program, even if all of the prerequisites are met. If items in this document are unclear or require further explanation, please contact your Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Program Office if further assistance is required.

When ready to submit a program application, APN Partners should complete the Partner Self-Assessment column of the checklist set forth in this document.

To submit your application:

1. Log in to the APN Partner Central (https://partnercentral.awspartner.com/), as Alliance Lead
2. Select "View My APN Account" from the left side of the page
3. Scroll to "Program Details" section
4. Select "Update" next to AWS Competency you wish to apply for
5. Fill out Program Application and Click "Submit"
6. Email completed Self-Assessment to competency-checklist@amazon.com. The Self-Assessment must include:
    - The Category of the solution (Cloud Governance or Resource & Cost Optimization)
    - Documentation for the four Case Studies (see definitions below)

If you have any questions regarding the above instructions, please contact your APN Partner Development Representative/Manager.

AWS will review and aim to respond back with any questions within five (5) business days to initiate scheduling of your validation or to request additional information.

APN Partners should prepare for the validation by reading the checklist, completing a self-assessment, and gathering and organizing the necessary documentation.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the validation. The best practice is for the APN Partner to make the following personnel available for the validation: one or more highly technical AWS engineers/architects who can speak about the submitted case studies applicable to this competency, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation.

Program Participation and Benefits

AWS may revoke an APN Partner's status as an AWS Competency Partner if at any time AWS determines in its sole discretion that such APN Partner does not meet the AWS Competency Program requirements or otherwise fails to represent the high standards expected of AWS Competency Partners. If an APN Partner's status as an AWS Competency Partner is revoked, such APN Partner will (i) no longer receive, and will immediately cease taking advantage of, any AWS Competency Partner Program benefits, (ii) immediately cease use of all materials provided to it in connection with the AWS Competency Partner Program and (iii) immediately cease to identify itself or hold itself out as an AWS Competency Partner.

Impact of Merger, Acquisition, and Divestiture Activity

The AWS Competency Program validates Partners solutions, as well as its business and delivery models. These business and delivery models are often significantly impacted in the process of mergers, acquisitions and divestitures. As a result, APN Partners may be required to reapply and complete a new audit based on the resulting businesses from their M&A activity. Please refer to the guidelines below.

Acquisition/Merger

Competency Partner acquires non-Competency Partner: No immediate action required. The Competency Partner should describe any impacts to its AWS Competency solution during any subsequent validation.

Non-Competency Partner acquires Competency Partner: New application and validation required for acquiring Partner to be recognized as an AWS Competency Partner. The new business and delivery models, as well as the integration of the acquired technical capabilities, must be validated through this process. We recommend that this be done as soon as possible to ensure continued recognition in the AWS Competency Program.

Competency Partner acquires another Competency Partner: No immediate action required. The consolidated entity will be assessed during the renewal for either of the original entities (whichever date is soonest).

Divestiture

Competency Partner divests a portion of its business related to its AWS Competency practice: The divesting business should immediately disclose significant impacts to its AWS Competency that would materially impact its standing as a Competency Partner. Depending on the significance of the impact, the APN Partner will either be immediately removed from the program or will be required to highlight impacts to the business during the next renewal. The divested business will be required to apply to the Competency Program as a new APN Partner.

Definitions

APN Partner Solution

APN Competencies are granted to partners offering a specific Partner Solution conforming to the requirements of an AWS Competency.

AWS Case Studies

All APN Partners will need to provide a number of AWS Case Studies detailing completed deployments of the Partner Solution. An AWS Case Study is a written description of a completed customer project that includes individual customer solutions and outcomes. Case Studies should include an introduction to the customer, overview of the challenge, details about the solution implemented, AWS services and additional 3rd Party tools leveraged, date delivered, and outcomes realized by the customer.

AWS Case Studies should be identified in writing to AWS as being either *public* (can be shared with public audiences) or *non-public* (can only be shared with AWS and its third-party auditor for the purpose of the audit or demonstrating to AWS that APN Partner meets program requirements). Once approved for an AWS Competency, *public* AWS Case Studies will be used on the AWS website to showcase partner-customer success.

AWS Business Requirements Validation

All APN Partners will undergo an AWS Business Requirements Validation in order to achieve an AWS Competency. Business Requirements Validations are an assessment that the APN Partner meets the non-technical requirements for the Competency, including the requirements for APN Advanced Tier standing, minimum numbers of suitable public and private AWS Case Studies, an AWS-specific landing page, and active engagement in thought leadership activities.

AWS Technical Validation

All APN Partners will undergo an AWS Technical Validation in order to achieve an AWS Competency. Technical Validations are assessments of an APN Partner Solution in the context of specific AWS Case Studies. Technical Validations confirm the APN Partner's capabilities in developing and delivering customer solutions using AWS Services specific to a solution area, workload, or vertical market while conforming with the AWS best-practices described in the AWS Well-Architected Framework. APN Partners demonstrate to 3rd-party Auditors and/or AWS Partner Solutions Architects what they've done specific to the AWS Case Studies submitted for the Competency.

Requirements for Technical Validations are fully documented in the competency-specific Technical Validation Checklist below. Each Technical Validation is comprised of three elements:

1. **Documentation Review**: APN Partners will be expected to provide technical documentation detailing the Partner Solution and each AWS Case Study provided. Third-party Auditors and/or AWS Partner Solutions Architects will use the documentation to confirm alignment with the requirements of the Competency as described in the checklist. The documentation is expected to consist of both public information (e.g. on- or offline deployment guides, installation manuals) and non-public information (e.g. architecture diagrams, design documents, and security assessments.) Public information will be assessed for alignment with best practices and the use of APN-approved marketing language. Non-public information may be anonymized at the APN Partner's discretion.
2. **Architecture Baseline Review**: APN Partners who configure or operate an AWS environment as part of the Partner Solution or AWS Case Study will undergo a competency-specific AWS Architecture Baseline Review of that environment. Requirements are based on the tenets of the AWS Well-Architected program and detailed in the checklist.
3. **Competency- and category-specific technical requirements**: Each competency and category is intended to highlight a specific solution that addresses a customer problem. As such, the checklist may include competency-specific requirements highlighting specific methodologies and capabilities the solution must provide to customer. Please see the checklist for more information.

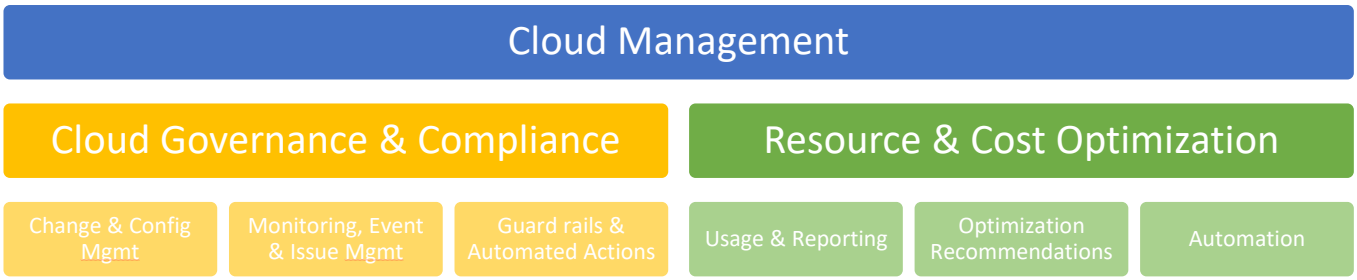
Elements of the APN Partner Solution or AWS Case Study that don't meet the requirements will be identified as 'Critical findings'. All Critical findings identified during the review will need to be remediated prior to achieving the Competency. If Critical findings relating to a specific AWS Case Study are unable to be remediated, the Case Study may be removed from consideration for inclusion in the competency.

Cloud Management Tools Competency Categories

APN Partners must also identify the Segment Category that their solution fits into:

1.) **Cloud Governance:** AWS workloads are synonymous with being highly immutable, agile and based on a micro services-architecture. This increases the management responsibilities to drive governance and compliance. Partner solutions in this category aim to simplify the management of AWS resources (infrastructure). They provide policy driven guardrails to track, report, alert and take action on configuration changes and non-compliant resources or actions. They easily integrate with AWS Management tools and external third party solutions to drive governance of a customer's cloud resources.

2.) **Resource & Cost Optimization:** AWS provides a level of cost visibility that is not available in traditional on-premises data centers. Partner solutions in this category help customers gain visibility into their AWS accounts and see exact workload costs, resource utilization, chargebacks, and more. Once cost visibility is achieved, partner solutions provide resource and cost optimization recommendations to help customers maximize their AWS investment. Leading solutions leverage machine learning and automation to simplify the management of cost and execution of optimization opportunities.



AWS Cloud Management Tools Competency Program Prerequisites

The following items will be validated by the AWS Competency Program Manager; missing or incomplete information must be addressed prior to scheduling of the Technology Validation Review.

1.0 APN Program Membership		Met Y/N
1.1 Technology Partner Tier	APN Partner must be an Advanced Tier APN Technology Partner before applying to the Cloud Management Tools Competency Program.	
1.2 Solution Category	APN Partner to identify the Segment Category for their solution: ☐ **Cloud Governance** ☐ **Resource & Cost Optimization** Deployment Model: ☐ **SaaS on AWS** ☐ **SaaS outside AWS** ☐ **BYOL on AWS** ☐ **BYOL On-premises**	
1.3 Customer Adoption	APN Partner to describe total number of customers leveraging their solution.	
2.0 Case Studies		**Met Y/N**
2.1 Cloud Management Tools-Specific Case Studies	APN Partner must have four (4) Case Studies specific to a Cloud Management Tools solution under review. It is acceptable for a partner solution to be comprised of multiple products to address a category use case. Each of the four Case Studies must relate to an example of the Partner Solution being used in one of the three Segment Categories (Admin & Provisioning, Cloud Governance and Resource & Cost Optimization). For each Case Study, the APN Partner must provide the following information: ▪ Name of the customer ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ Third party applications or solutions used ▪ Date the reference entered production ▪ Outcome(s)/results ▪ Specific Architecture Diagrams, Deployment Guides and other materials depending on the type of solution, as described in the next section. This information will be requested as part of the Program Application process in APN Partner Central. The information provided as part of this Case Study can be private and will not be made public. All four of the Case Studies provided will be examined in the Documentation Review of the Technical Validation. The Case Study will be removed from consideration for inclusion in the Competency if the Partner cannot provide the documentation necessary to assess the Case Study against each checklist item, or if there were any of the checklist items are not met. Case Studies must describe deployments that have been performed within the past 18 months, and must be for projects that are in production with customers, rather than in a 'pilot' or proof of concept stage.	
2.2 Publicly Available Case Studies	Publicly available case studies are used by AWS upon approval into the Competency to showcase the Partner's demonstrated success based on measurable KPIs with the solution and provide customers with confidence that the APN Partner has the experience and knowledge needed to develop and deliver solutions to meet their objectives. Two (2) of the four (4) customer deployments associated with the Case Studies must be publicized by the APN Partner as publicly available case studies. These publicly available case studies may in the form of formal case studies, white papers, videos, or blog posts.	
	Publicly available case studies must be easily discoverable from the APN Partner's website, e.g. it must be possible to navigate to the publicly available case study from the Partner's home page,	

	and the APN Partner must provide links to these publicly available case studies in their application. Publicly available case studies must include the following: ▪ References to the customer name, APN Partner name, and AWS ▪ Customer challenge ▪ How the solution was deployed to meet the challenge ▪ How AWS services were used as part of the solution ▪ Outcome(s)/results	
3.0 AWS Cloud Management Web Presence and Thought Leadership		**Met Y/N**
3.1 Partner AWS Landing Page	An APN Partner's internet presence specific to their AWS Cloud Management Tools Solutions provides customers with confidence about the APN Partner's capabilities and experience. APN Partner must have an AWS Landing Page that describes their AWS Cloud Management Tools solution, links to their publicly available case studies, lists technology partnerships, and provides any other relevant information supporting the Partner's expertise related to Cloud Management and highlighting the partnership with AWS. This AWS-specific CMT page must be accessible from the APN Partner's home page. The home page itself is not acceptable as an AWS Landing Page unless APN Partner is a dedicated CMT company and home page reflects APN Partner's focus on Cloud Management.	
3.2 Cloud Management Thought Leadership	AWS CMT Competency Partners are viewed as having deep domain expertise in Cloud Management, having developed innovative solutions that leverage or help manage AWS services. APN Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the APN Partner's focus on and expertise in Cloud Management. Links must be provided to examples of materials published within the last 12 months.	
4.0 Business Requirements		
4.1 Field-Ready Toolkits	APN Partner has field-ready documentation and seller toolkits including a clear product value proposition that can be articulated to the AWS sales organization with all relevant information needed to determine fit for a customer opportunity (e.g., sales collateral, presentation, and customer use cases). Evidence must be in the form of sales collateral including a presentation, one-pager, and use-case checklist.	
4.2 Product Support/Help Desk	APN Partner offers product support via web chat, phone, or email support to customers. Evidence must be in the form of description of support offered to customers for their product or solution.	
4.3 Product is listed on AWS Marketplace	APN Partner makes solution available via AWS Marketplace. ☐ Yes ☐ No If "yes", APN Partner must provide a link to the AWS Marketplace listing. If "no", no further information is required. Note, AWS Marketplace is not mandatory to achieve the competency	
5.0 APN Partner Self-Assessment		**Met Y/N**
5.1 AWS Competency Partner Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment of their compliance to the requirements of the AWS CMT Technology Partner Validation Checklist. ▪ APN Partner must complete all sections of the checklist. ▪ Completed self-assessment must be emailed to **competency-checklist@amazon.com**, using the following convention for the email subject line: "[APN Partner Name], Cloud Management Tools Competency Technology Partner Completed Self-Assessment." ▪ It is recommended that APN Partner has their Partner Solutions Architect, Partner Development Representative (PDR), or Partner Development Manager (PDM) review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the APN Partner's AWS team is engaged and working to provide recommendations prior to the review and to help ensure a productive review experience.	

CMT Competency Technology Partner Validation Checklist

The following items will be validated by the Third-party Auditors and/or AWS Partner Solutions Architects; missing or incomplete information must be addressed prior to scheduling of the Technology Validation Review.

CMT Technical Requirements		Met Y/N
Required Solution Features Documentation describing how the partner solution meets the requirements must be submitted as part of the competency self-assessment		
Cloud Governance	Ability to monitor AWS Resources for governance and policy management based on AWS best practices, industry best practices and customers unique needs	
	Implement guardrails to manage account/resource configurations. Solution should provide flexibility to modify guardrails based on specific needs (rules based events)	
	Provide guidance, or manage, AWS service limits. Solutions in this category often use describe API's that are limited based on the service and region. Solution should have a method for managing and addressing the different service limits to deliver a consistent customer experience	
	When a non-compliant event occurs, solution provides ability to send alerts, manually remediate or automatically remediate	
	Provide visibility into AWS resource types and configurations. Maintain configuration compliance by tracking configuration drift, anomalies, etc. Integration between AWS Config and/or AWS Systems Manager with central IT CMDB for resource management is a best practice	
	Integrate with AWS CloudTrail, Config or CloudWatch to provide near real time alerts and notification for **infrastructure** incidents. Solution must demonstrate how it integrates with AWS Management tools to help customers quickly identify and remediate issues. Use of advanced AI/ML algorithms to help simplify infrastructure event and incident management is a best practice	
	Ability to monitoring overall performance health of AWS resources. Integration with CloudWatch, Personal Health Dashboard and Trusted Advisor are best practices	
Resource and Cost Optimization	Provides standard cost management features such as cost trending, predictive analysis, budget vs actual spend, charge back, resource utilization, spend alerts, untagged/misspelled resources, etc	
	Ability to manage complex, multi-region, multi-account environments	
	Provide cost optimization recommendations such as resource utilization, instance right sizing, storage type recommendations, unattached storage, etc	
	Provides Reserved Instance recommendations and management	
	Provides SPOT recommendations and management	
	Provides highly flexible reporting including fixed and custom views	
	Provides option to automatically remediate/implement optimization recommendations	
	Solutions must leverage the AWS Cost and Usage report	
	Global pre and post-sales support beyond basic setup and configuration	

Technical Validation		Applies to: Multi-tenant SaaS	Single-tenant SaaS	Customer Deployed On-Premises	Customer-Deployed on AWS	Met Y/N
Required Documentation All of the following documentation must be submitted as part of the Competency Self-Assessment.						
Architecture Diagram	Depending on the Deployment Category, one or more Architecture Diagrams are required. Each Architecture Diagram must show: ☐ The major elements of the architecture, and how they combine to provide the Partner Solution to customers ☐ All of the AWS services used, using the appropriate AWS service icons. ☐ How the AWS services are deployed, including, VPCs, AZs, subnets, and connections to systems outside of AWS. ☐ Includes elements deployed outside of AWS, e.g. on-premises components, or hardware devices.	Yes – one for the whole solution and one for each Case Study.	Yes – one for the whole solution and one for each Case Study.	Yes – one for each Case Study.	Yes – one for each Case Study.	
Deployment Guide	The Deployment Guide must provide best practices for deploying the Partner Solution on AWS, and include all of the sections outlined in "Baseline Requirements for Deployment Guides"	No	No	No	Yes – one for the solution.	
Completed Validation Checklist	For each of the four Case Studies provided for the Partner Solution, the APN Partner must provide a completed version of the following checklist indicating which checklist items are met.	Yes	Yes	Yes	Yes	
1.0 Security The security pillar focuses on protecting information & systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.						
1.1 AWS account root user is not used for routine activities	The AWS account root user must not be used for routine activities. Following the creation of your AWS account, you should immediately create IAM user accounts, and use these IAM user accounts for all routine activities. Once your IAM users accounts have been created, you should securely store the AWS root account credentials and use them only to perform the few account and service management tasks that require the AWS account root user. For further information on how to set up an	Yes	Yes	No	No	

	IAM user accounts and groups for daily use, see Creating Your First IAM Admin User and Group.					
1.2 Multi-Factor Authentication (MFA) has been enabled on the AWS account root user	MFA must be enabled for your AWS account root user. Because your AWS account root user can perform sensitive operations in your AWS account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available, including virtual MFA and hardware MFA.	Yes	Yes	No	No	
1.3 IAM user accounts used for all routine activities	The AWS account root user must not be used for any task where it is not required. Instead, create a new IAM user for each person that requires administrator access. Then make those users administrators by placing the users into an Administrators group to which you attach the AdministratorAccess managed policy. Thereafter, the users in the administrators group should set up the groups, users, and so on, for the AWS account. All future interaction should be through the AWS account's users and their own keys instead of the root user. However, to perform some account and service management tasks, you must log in using the root user credentials.	Yes	Yes	No	No	
1.4 Multi-Factor Authentication (MFA) is enabled for all interactive IAM users	You must enable MFA for all interactive IAM users. With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).	Yes	Yes	No	No	
1.5 IAM credentials are rotated regularly	You must change your passwords and access keys regularly, and make sure that all IAM users in your account do as well. That way, if a password or access key is compromised without your knowledge, you limit how long the credentials can be used to access your resources. You can apply a password policy to your account to require all your IAM users to rotate their passwords, and you can choose how often they must do so. For more information about rotating access keys for IAM users, see Rotating Access Keys.	Yes	Yes	Yes (for credentials used to integrate with AWS)	Yes (for credentials used to integrate with AWS)	
1.7 Strong password policy is	You must configure a strong password policy for your IAM	Yes	Yes	Yes (for credentials used	Yes (for credentials	

in place for IAM users	users. If you allow users to change their own passwords, require that they create strong passwords and that they rotate their passwords periodically. On the Account Settings page of the IAM console, you can create a password policy for your account. You can use the password policy to define password requirements, such as minimum length, whether it requires non-alphabetic characters, how frequently it must be rotated, and so on. For more information, see Setting an Account Password Policy for IAM Users.			to integrate with AWS)	used to integrate with AWS)	
1.8 IAM credentials are not shared among multiple users	You must create an individual IAM user account for anyone who needs access to your AWS account. Create an IAM user for yourself as well, give that user administrative privileges, and use that IAM user for all your work. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time. (If you give out your root user credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)	Yes	Yes	No	No	
1.9 IAM policies are scoped down to least privilege	You must follow the standard security advice of granting least privilege. This means granting only the permissions required to perform a task. Determine what users need to do and then craft policies for them that let the users perform only those tasks. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. Defining the right set of permissions requires some research. Determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.	Yes	Yes	Yes (for solutions ran outside of AWS integrated via IAM roles, least privilege access should be applied)	Yes (for solutions ran outside of AWS integrated via IAM roles, least privilege access should be applied)	
1.10 Hard-coded credentials (e.g. access keys) are not used	You must follow best practices for managing AWS access keys and avoid the use of hard-coded credentials. When you access AWS programmatically, you use an	Yes	Yes	Yes (credentials used to integration with AWS should be easily changed	Yes (credentials used to integration with AWS	

	access key to verify your identity and the identity of your applications. Anyone who has your access key has the same level of access to your AWS resources that you do. Consequently, AWS goes to significant lengths to protect your access keys, and, in keeping with our shared responsibility model, you should as well.			and not hard coded)	should be easily changed and not hard coded)	
1.11 All credentials are encrypted at rest	The baseline requirement is to ensure the encryption of any credentials at rest.	Yes	Yes	Yes (credentials stored in partner solution used to integrate with AWS should be encrypted)	Yes (credentials stored in partner solution used to integrate with AWS should be encrypted)	
1.12 AWS Access Keys only used by interactive users	No AWS Access Keys should be in use, except in the following cases: 1. Used by humans to access AWS services, and stored securely on a device controlled by that human. 2. Used by a service to access AWS services, but only in cases where: a) It is not feasible to use an EC2 instance role, ECS Task Role or similar mechanism, b) The AWS Access Keys are rotated at least weekly, and c) The IAM Policy is tightly scoped so that it: i) Allows only access to only specific methods and targets and ii) Restricts access to the subnets on from which the resources will be accessed.	Yes	Yes	No	No	
1.13 CloudTrail is enabled for all AWS accounts in every region	CloudTrail must be enabled on all AWS accounts and in every region. Visibility into your AWS account activity is a key aspect of security and operational best practices. You can use CloudTrail to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure.You can identify who or what took which action, what resources were acted upon, when the event occurred, and other details to help you analyze and respond to activity in your AWS account.	Yes	Yes	No	No	
1.14 CloudTrail logs are stored in an S3 bucket owned by another AWS account	CloudTrail logs must be emplaced in a bucket owned by another AWS account configured for extremely limited access, such as audit and recovery only.	Yes	Yes	No	No	
1.15 CloudTrail S3 log bucket has Versioning or MFA Delete enabled	CloudTrail log bucket contents must be protected with versioning or MFA Delete.	Yes	Yes	No	No	

1.16 EC2 security groups are tightly scoped	All EC2 security groups should restrict access to the greatest degree possible. This includes at least 1. Implementing Security Groups to restrict traffic between Internet and VPC, 2. Implementing Security Groups to restrict traffic within the VPC, and 3. In all cases, allow only the most restrictive possible settings.	Yes	Yes	No	Yes	
1.17 S3 buckets within your account have appropriate levels of access	You must ensure that the appropriate controls are in place to control access to each S3 bucket. When using AWS, it's best practice to restrict access to your resources to the people that absolutely need it (the principle of least privilege).	Yes	Yes	No	No (unless partner solution running on AWS requires the S3 service)	
1.18 S3 buckets have not been misconfigured to allow public access.	You must ensure that buckets that should not allow public access are properly configured to prevent public access. By default, all S3 buckets are private, and can only be accessed by users that have been explicitly granted access. Most use cases won't require broad-ranging public access to read files from your S3 buckets, unless you're using S3 to host public assets (for example, to host images for use on a public website), and it's best practice to never open access to the public.	Yes	Yes	No	No (unless partner solution running on AWS requires the S3 service)	
1.19 A monitoring mechanism is in place to detect when S3 buckets or objects become public	You must have monitoring or alerting in place to identify when S3 buckets become public. One option for this is to use Trusted Advisor. Trusted Advisor checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions. Bucket permissions that grant List access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket. The Trusted Advisor check examines explicit bucket permissions and associated bucket policies that might override the bucket permissions.	Yes	Yes	Yes	No (unless partner solution running on AWS requires the S3 service)	
1.20 A monitoring mechanism is in place to detect changes in EC2 instances and Containers	Any changes to your EC2 instances or Containers may indicate unauthorized activity, and must at a minimum be logged to a durable location to allow for future forensic investigation. The mechanism employed for this purpose must at least: 1. Detect	Yes	Yes	No	No	

	any changes to the OS or application files in the EC2 instances or Containers used in the solution. 2 Store data recording these changes in a durable location, external to the EC2 instance or Container. Examples of suitable mechanisms include: a. Deployment of file integrity checking via scheduled configuration management (e.g. Chef, Puppet, etc.) or a specialized tool (e.g. OSSEC, Tripwire or similar), or b. Extending configuration management tooling to validate EC2 host configuration, and alert on updates to key configuration files or packages with 'canary' (logged no-op) events configured to ensure the service remains operational on all in-scope hosts during runtime, or c. Deploying a Host Intrusion Detection System such as an open source solution like OSSEC with ElasticSearch and Kibana or using a partner solution. Note that the following mechanism does not meet this requirement: a. Frequently cycling EC2 instances or Containers.					
1.21 All data is classified	All customer data processed and stored in the workload is considered and classified to determine its sensitivity and the appropriate methods to use when handling it.	Yes	Yes	No	No	
1.22 All sensitive data is encrypted	All customer data classified as sensitive is encrypted in transit and at rest.	Yes	Yes	No	No	
1.23 Cryptographic keys are managed securely	All cryptographic keys are encrypted at rest and in transit, and access to use the keys is controlled using an AWS solution such as KMS or a partner solution such as HashiCorp Vault.	Yes	Yes	Yes	Yes	
1.24 All data in transit is encrypted	All data in transit across a VPC boundary is encrypted.	Yes	Yes	Yes	Yes	
1.25 Security incident response process is defined and rehearsed	A security incident response process must be defined for handling incidents such as AWS account compromises. This process must be tested by implementing procedures to rehearse the incident response process, e.g. by completing a security game day exercise. A rehearsal must have been held within the last 12 months to confirm that: a. The appropriate people have access to the environment. b. The appropriate tools are available. c. The appropriate people know what to	Yes	Yes	No	No	

	do to respond to the various security incidents outlined in the plan.					
2.0 Reliability The reliability pillar focuses on the ability to prevent, and quickly recover from failures to meet business and customer demand. Key topics include foundational elements around setup, cross project requirements, recovery planning, and how we handle change.						
2.1 Network connectivity is highly available	Network connectivity to the solution must be highly available. If using VPN or Direct Connect to connect to customer networks, the solution must support redundant connections, even if the customers do not always implement this.	Yes	Yes	Yes	Yes	
2.2 Infrastructure scaling mechanisms align with business requirements	Infrastructure scaling mechanisms must align with business requirements, either by: 1. Implementing auto-scaling mechanisms at each layer of the architecture, by 2. Confirming that current business requirements, including cost requirements and anticipated user growth, do not require auto-scaling mechanisms AND manual scaling procedures are fully documented and frequently tested.	Yes	Yes	No	Yes	
2.3 AWS and Application logs are managed centrally	All log information from the application, and from the AWS infrastructure, should be consolidated into a single system.	Yes	Yes	No	No	
2.4 AWS and Application monitoring and alarms are managed centrally	The application and the AWS infrastructure must be monitored centrally, with alarms generated and sent to the appropriate operations staff.	Yes	Yes	No	No	
2.5 Infrastructure provisioning and management is automated	The solution must use an automated tool such as CloudFormation or Terraform to provision and manage the AWS infrastructure. The AWS Console must not be used to make routine changes to the production AWS infrastructure.	Yes	Yes	No	No	
2.6 Regular data backups are being performed	You must perform regular backups to a durable storage service. Backups ensure that you have the ability to recover from administrative, logical, or physical error scenarios. Amazon S3 and Amazon Glacier are ideal services for backup and archival. Both are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. The pay-for-what-you-use model and low cost per GB/month make these services a good fit for data protection use cases.	Yes	Yes	No	No	
2.7 Recovery mechanisms are	You must test recovery mechanisms and procedures, both	Yes	Yes	No	No	

being tested on a regular schedule and after significant architectural changes	on a periodic basis and after making significant changes to your cloud environment. AWS provides substantial resources to help you manage backup and restore of your data.					
2.8 Solution is resilient to availability zone disruption	The solution must continue to operate in the case where all of the services within a single availability zone have been disrupted.	Yes	Yes	No	Yes	
2.9 Resiliency of the solution has been tested	The resiliency of the infrastructure to disruption of a single availability zone has been tested in production, e.g. through a game day exercise, within the last 12 months.	Yes	Yes	No	Yes	
2.10 Disaster Recovery (DR) plan has been defined	A well-defined Disaster Recovery plan includes a Recovery Point Objective (RPO) and a Recovery Time Objective (RTO). You must define an RPO and an RTO for all in-scope services, and the RPO and RTO must align with the SLA you offer to your customers	Yes	Yes	No	No	
2.11 Recovery Time Objective (RTO) is less than 24 hours	The baseline requirement is for the RTO to be less than 24 hours for core services.	Yes	Yes	No	No	
2.12 Disaster Recovery (DR) plan is adequately tested	Your DR plan must be tested against your Recovery Point Objective (RPO) and Recovery Time Objective (RTO), both periodically and after major updates. At least one DR test must be completed prior to approval of your AWS APN Advanced Tier application.	Yes	Yes	No	No	
2.13 Disaster Recovery (DR) plan includes recovery to another AWS account	Your DR plan must include a strategy for recovering to another AWS account, and your periodic recovery testing must test this scenario. You must have completed at least one full test of the DR plan, including at least recovery to another AWS account, within the last 12 months. Note: Although processes restoring data into test environments or exporting data for users are useful ways to verify backups, these processes do not fulfill the requirement to perform a full restore test to another AWS account.	Yes	Yes	No	No	
3.0 Operational Excellence The operational excellence pillar focuses on running and monitoring systems to deliver business value, and continually improving processes and procedures. Key topics include managing and automating changes, responding to events, and defining standards to successfully manage daily operations.						
3.1 Deployment of code changes is automated	The solution must use an automated method of deploying code to the AWS infrastructure. Interactive SSH or RDP sessions	Yes	Yes	No	No	

	must not be used to deploy updates in the AWS infrastructure.					
3.2 Runbooks and escalation process are defined	Runbooks must be developed to define the standard procedures used in response to different application and AWS events. An escalation process must be defined to deal with alerts and alarms generated by the system, and to respond to customer-reported incidents. The escalation process must also include escalating to AWS Support where appropriate.	Yes	Yes	No	No	
3.3 AWS Business Support is enabled for the AWS Account	Business Support must be enabled. Business Support (or greater) is an AWS Partner Network requirement for Advanced Tier Technology Partners. To qualify for Advanced Tier, you must enable Business Support on at least one of your AWS accounts.	Yes	Yes	No	No	

AWS Resources:

AWS Well Architected Website
https://aws.amazon.com/architecture/well-architected/

AWS Whitepapers
https://aws.amazon.com/whitepapers/

APN Blog
https://aws.amazon.com/blogs/apn/

AWS Blog
https://aws.amazon.com/blogs/